**UNITED STATES DISTRICT COURT**
**NORTHERN DISTRICT OF TEXAS**
**DALLAS DIVISION**

| | |
|---|---|
| JENNIFER TURNER, individually, and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>AT&T, INC.,<br><br>Defendant. | CIVIL ACTION NO. _____<br><br>**DEMAND FOR JURY TRIAL** |

# CLASS ACTION COMPLAINT

Plaintiff Jennifer Turner ("Plaintiff") by and through her undersigned attorneys, individually, and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant AT&T, Inc. ("AT&T" or "Defendant") and makes the following allegations based upon knowledge as to herself and her own acts, and upon information and belief as to all other matters, as follows:

## INTRODUCTION

1. This is a class action brought by Plaintiff individually, and on behalf of all other similarly situated individuals whose personal information, including names, email addresses, mailing addresses, phone numbers, social security numbers, dates of birth, AT&T account numbers and passcodes (hereinafter "Personal Information" or "PI") was stolen from AT&T and leaked on the Dark Web (the "Data Breach").

2. Upon information and belief, AT&T collects and maintains the sensitive information of its customers, like the Personal Information at issue in the Data Breach.

3. On or around March 30, 2024, AT&T confirmed that the Personal Information of approximately 7.6 million current customers and 65.4 million former account holders, or

approximately 73 million total customers, was leaked on the Dark Web approximately two weeks prior.[1] While AT&T has reported that its investigation is ongoing, AT&T has determined that "AT&T data-specific fields were contained in a data set released[,]" but maintains that "it is not yet known whether the data in those fields originated from AT&T or one of its vendors."[2]

4. As a result of Defendant's misconduct and the Data Breach, the Personal Information of approximately 73 million Americans who had entrusted their sensitive information to Defendant has been exposed. Victims have had their Personal Information compromised, their privacy violated, are at an increased risk of exposure to fraud and identity theft, have suffered a loss of control over their personal and financial information, and have otherwise been injured. Through this suit, Plaintiff and the Class seek to recover damages caused by Defendant's breaches of common law duties and violations of other laws. Plaintiff also seeks injunctive and declaratory relief on behalf of themselves and similarly situated Class members.

## PARTIES

5. **Plaintiff Jennifer Turner** is a resident of California. Plaintiff Turner was a AT&T cellular phone account holder from approximately 2016 to approximately May 2023. Upon learning of the Data Breach, Ms. Turner was concerned that her Personal Information was leaked on Dark Web. Since AT&T's customers' information first appeared on the Dark Web, Ms. Turner has experienced several issues, including account take overs and issues with her bank accounts and credit card fraud. Ms. Turner has had to spend time to remedy these issues as well as continue to monitor for fraud. As a result of Defendant's failures to adequately safeguard Plaintiff's Personal Information, Plaintiff has been injured.

---

[1] *See* https://www.att.com/support/article/my-account/000101995?bypasscache=1/?source=EPcc000000000000U (last visited April 4, 2024).

[2] *Id.*

6. **Defendant AT&T, Inc.** is a Delaware corporation with its corporate headquarters at 208 South Akard Street, Dallas, Texas 75202. AT&T is a publicly traded company that provides wireless network, cell phone, digital television, internet, and landline telecommunication services to consumers throughout the United States. Defendant may be served through its registered agent CT Corporation System, 1999 Bryan St., Ste. 900, Dallas, TX 75201-3136 USA.

## JURISDICTION

7. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5,000,000, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of different states than Defendant. *See* 28 U.S.C. § 1332(d)(2)(A). This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

8. This Court has personal jurisdiction over AT&T because it is headquartered in Texas, is authorized to and conducts business in Texas, has specifically marketed, advertised, and made substantial revenue in Texas, and has sufficient minimum contacts with this state and/or sufficiently avails itself of the markets of this state through its promotion, revenue, and marketing within this state to render the exercise of jurisdiction by this Court permissible.

9. Venue in this Court is proper pursuant to 28 U.S.C. § 1391 because Defendant does substantial business in this District, has intentionally availed itself of the laws and markets within this District through its promotion, marketing, and business activities in this District, and a significant portion of the facts and circumstances giving rise to Plaintiff's Complaint occurred in or emanated from this District.

## FACTUAL ALLEGATIONS

### A. The Data Breach

10. In or around March 2024, AT&T confirmed that the Personal Information and sensitive details of approximately 7.6 million current customers and 65.4 million former account holders, or approximately 73 million total customers was leaked on the Dark Web.[3] The Personal Information possibly included, for each customer, "a person's full name, email address, mailing address, phone number, Social Security number, date of birth, AT&T account number and passcode."[4]

11. According to news reports, "[d]etails of the leaked data first appeared online in August 2021, when a known threat actor, ShinyHunters, offered up the records for sale on a hacking forum, with a 'buy it now' price of one million dollars."[5] Then, in March 2024, "that same data appears to have been made available for free by another threat actor, MajorNelson."[6] Sometime after that information became available again on the Dark Web, AT&T issued a press release addressing the Data Breach.[7]

> This is the first time since the Personal Information first appeared in 2021 that AT&T has admitted that the Personal Information was its customers' information. "Back in August 2021, when the information was first made available for sale, it was claimed to have come from an AT&T data breach, which seems the most obvious conclusion. However, at the time, AT&T denied all

[3] *See* https://www.nytimes.com/2024/03/30/business/att-passcodes-reset-data-breach.html (last visited April 4, 2024).

[4] *Id.*

[5] *See* https://tech.co/news/att-accounts-leaked-70-million-check#:~:text=AT%26T%20Customer%20Data%20for%20Sale&text=Details%20of%20the%20leaked%20data,price%20of%20one%20million%20dollars. (last visited April 4, 2024).

[6] *Id.*

[7] *See* https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html (last visited April 4, 2024).

> knowledge, telling Bleeping Computer that the data did 'not appear' to have come from their systems."[8]

12. Now, in its announcement regarding the Data Breach, AT&T stated that "AT&T has determined that AT&T data-specific fields were contained in a data set released on the [D]ark [W]eb. While AT&T has made this determination, it is not yet known whether the data in those fields originated from AT&T or one of its vendors."[9]

13. AT&T further stated that:

> [it] "has come to our attention that a number of AT&T passcodes have been compromised. We are reaching out to all 7.6M impacted customers and, as a safety precaution, have reset their passcodes. In addition, we are emailing and mailing letters to individuals with compromised sensitive personal information separately and offering complimentary identity theft and credit monitoring services."[10]

14. While AT&T stated that its "internal teams are working with external cybersecurity experts to analyze the situation" and that "[t]o the best of our knowledge, the compromised data appears to be from 2019 or earlier and does not contain personal financial information or call history" it is still encouraging customers to "remain vigilant by monitoring account activity and credit reports, as well as being mindful of phishing scams."[11] This is despite offering complimentary identity theft and credit monitoring services to affected individuals.[12]

15. Glaringly, AT&T will still not admit that they know where the Personal Information came from, with a spokesperson stating that "[w]e have no indications of a compromise of our

---

[8] *See* https://tech.co/news/att-accounts-leaked-70-million-check#:~:text=AT%26T%20Customer%20Data%20for%20Sale&text=Details%20of%20the%20leaked%20data,price%20of%20one%20million%20dollars. (last visited April 4, 2024).

[9] *See* https://www.att.com/support/article/my-account/000101995?bypasscache=1/?source=EPcc000000000000U (last visited April 4, 2024).

[10] *Id.*

[11] *Id.*

[12] *Id.*

systems. We determined in 2021 that the information offered on this online forum did not appear to have come from our systems. This appears to be the same dataset that has been recycled several times on this forum."[13] However, "[i]nvestigating data breaches and leaks takes time. But by now AT&T should be able to provide a better explanation as to why millions of its customers' data is online for all to see."[14]

16. Notably, this isn't the first data breach AT&T has dealt with. "The Associated Press reports that the telecom company has experienced several breaches over the years, including one in 2014 where a rogue employee accessed personal data on about 1,600 customers."[15]

17. The fact that AT&T has dealt with other data breaches, has known that the Personal Information at issue first appeared on the Dark Web in 2021, and is only now admitting that that information belongs to its customers, makes this breach particularly egregious.

**B. AT&T's Privacy Policies**

18. AT&T states through its website that "[y]our privacy is important to you and us."[16] Further, AT&T states that

> "[y]ou can count on us to provide you with products and services designed with privacy in mind, while also giving you control over how your information is shared. Our Privacy Center explains our approach to privacy and data use in simple language, and presents you with helpful links to privacy choices, security tips, and much more."[17]

---

[13] *See* https://techcrunch.com/2024/03/22/att-customers-data-leak-online/ (last visited April 4, 2024).

[14] *Id.*

[15] *See* https://money.com/att-data-breach/#:~:text=%E2%80%9CThe%20company%20is%20communicating%20proactively,typically%20four%20digits%20in%20length. (last visited April 4, 2024).

[16] *See* https://about.att.com/privacy/privacy-notice.html (last visited April 4, 2024).

[17] *See* https://about.att.com/privacy.html (last visited April 4, 2024).

19. Even further, AT&T states that "[o]ur Privacy Principles are fundamental to our business, and reflect our commitment to" transparency, choices and controls, security, and integrity.[18]

20. Despite these representations and agreements with consumers, AT&T failed to disclose that they did not maintain account holders' Personal Information in compliance with state and federal mandated data security protocols, or even industry standards, in order to prevent the unauthorized access, use, and theft of Personal Information.

### C. AT&T Failed to Comply with Industry and Regulatory Standards

21. Because of the value of Personal Information to cybercriminals and identity thieves, companies in the business of storing, maintaining, and securing Personal Information, such as AT&T, have been identified as being particularly vulnerable to cyber-attacks. Cybersecurity firms have promulgated a series of best practices that, at minimum, should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.[19]

22. Further, federal and state governments have likewise established security standards and issued recommendations to diminish data breaches and the resulting harm to consumers and financial institutions.

---

[18] *Id.*

[19] *See White Paper: Addressing BPO Information Security: A Three-Front Approach*, DATAMARK, Inc. (Nov. 2016), https://insights.datamark.net/addressing-bpo-information-security/.

23. Defendant was prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. § 45) from engaging in unfair or deceptive acts or practices in or affecting commerce. The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

24. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

25. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*,[20] which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

26. The FTC further recommends that companies not maintain PI longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

[20] *See* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (last visited April 4, 2024).

27. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

28. Defendant failed to properly implement these basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Personal Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

**D. Plaintiff's Experiences**

29. Plaintiff Turner learned of the Data Breach in or around April 2024.

30. As a result of learning of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes, but is not limited to: checking and verifying credit agency reports; changing passwords on accounts; checking and verifying Social Security accounts; and checking and verifying financial accounts for fraudulent activity.

31. Plaintiff suffered actual injury in the form of damages to and diminution of the value of Personal Information—a form of intangible property that Plaintiff entrusted to Defendant which was compromised in and as a result of the Data Breach.

32. Plaintiff has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach. This is time Plaintiff otherwise would have spent performing other activities, such as work and/or leisurely activities for the enjoyment of life.

33. Plaintiff has suffered imminent and impending injury arising from the disclosure of her Personal Information and for the substantially increased risk of fraud, identity theft, and misuse

resulting from Personal Information being placed in the hands of unauthorized third parties and criminals.

34. Plaintiff has a continued interest in ensuring that Personal Information, which remains backed up and in Defendant's possession, be protected and safeguarded from further and future breaches.

**E. Plaintiff and Class Members Suffered Damages**

35. Defendant had a duty to keep Personal Information confidential and to protect it from unauthorized access and disclosures. Plaintiff and Class Members provided their Personal Information to Defendant with the understanding that Defendant and any business partners to whom Defendant disclosed Personal Information would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

36. The Data Breach creates a heightened security concern for customers of Defendant because their Personal Information, including Social Security numbers and other sensitive personal data was involved in the Data Breach.

37. What's more, it took three years from the time Defendant learned that its customers' Personal Information was leaked on the Dark Web for individuals who were affected to be notified about it. Then, when its customers' Personal Information appeared on the Dark Web again, it failed to properly take responsibility for the Data Breach and adequately notify its customers.

38. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or

government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id.*

39. Theft of Social Security numbers creates a particularly alarming situation for victims because those numbers cannot easily be replaced. Indeed, the Social Security Administration stresses that the loss of an individual's Social Security number can lead to identity theft and extensive fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[21]

40. It is also difficult to obtain a new Social Security number. A breach victim would have to demonstrate ongoing harm from misuse of her Social Security number, and a new Social Security number will not be provided until after the harm has already been suffered by the victim.

41. Given the highly sensitive nature of Social Security numbers, theft of these numbers in combination with other personally identifying information may cause damage to victims for years.

42. Defendant had a duty to keep Personal Information confidential and to protect it from unauthorized disclosures. Plaintiff and Class Members provided their Personal Information to Defendant with the understanding that Defendant and any business partners to whom Defendant disclosed Personal Information would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

---

[21] *See Identity Theft and Your Social Security Number*, Social Security Administration, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited April 4, 2024).

43. Defendant's data security obligations were particularly important given the substantial increases in data breaches in recent years, which are widely known to the public and to anyone in Defendant's industry.

44. Data breaches are not new. These types of attacks should be anticipated by companies that store sensitive and personally identifying information, and these companies must ensure that data privacy and security is adequate to protect against and prevent known attacks. Indeed, many companies have been subject to numerous data security incidents, including AT&T in the past.

45. It is well known among companies that store sensitive personally identifying information that sensitive information is valuable and frequently targeted by criminals.

46. Identify theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, tax fraud, phone or utilities fraud, and bank/finance fraud.

47. There may be a time lag between when the harm occurs versus when it is discovered, and also between when Personal Information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[22]

[22] *See Report to Congressional Requesters*, U.S. Government Accountability Office, (June 2007), http://www.gao.gov/new.items/d07737.pdf. (last visited April 4, 2024).

48. With access to an individual's Personal Information, criminals can commit all manners of fraud, including obtaining a driver's license or official identification card in the victim's name but with the thief's picture, using the victim's name and Social Security number to obtain government benefits, or filing a fraudulent tax return using the victim's information.

49. Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web and the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen Social Security numbers and other Personal Information directly on various illegal websites making the information publicly available, often for a price. In fact, and as alleged above, AT&T already admitted that its customers' Personal Information was on the Dark Web.

50. Defendant is, and at all relevant times has been, aware that the Personal Information it handles and stores in connection with providing communications services is highly sensitive. As a company that handles highly sensitive and identifying Personal Information, Defendant is aware of the importance of safeguarding that information and protecting its systems and products from security vulnerabilities.

51. Despite the known risk of data breaches and the widespread publicity and industry alerts regarding other notable data breaches, Defendant failed to take reasonable steps to adequately protect its systems from being breached leaving its customers exposed to the risk of fraud and identity theft.

52. As a result of the events detailed herein, Plaintiff and Class Members suffered harm and loss of privacy, and will continue to suffer future harm, resulting from the Data Breach, including but not limited to: invasion of privacy; loss of privacy; loss of control over personal

information and identities; disclosure of their need for special education; disclosure of financial status; fraud and identity theft; unreimbursed losses relating to fraud and identity theft; loss of value and loss of possession and privacy of Personal Information; harm resulting from damaged credit scores and information; loss of time and money preparing for and resolving fraud and identity theft; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized exposure of Personal Information.

53. As a result of the Data Breach, Plaintiff's and Class Members' privacy has been invaded, their Personal Information is now in the hands of criminals, they face a substantially increased risk of identity theft and fraud, and they must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

54. Had Defendant remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiff's and Class Members' Personal Information.

55. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

56. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a

month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[23]

57. In its announcement, Defendant stated that it would offer credit monitoring at its expense where applicable. Defendant also encouraged customers to remain vigilant by monitoring account activity and credit reports, as well as being mindful of phishing scams.

58. Defendant's failure to adequately protect Plaintiff's and Class Members' Personal Information has resulted in Plaintiff and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money.

59. Defendant's offer of identity monitoring to Plaintiff and Class Members is inadequate. While some harm has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personal Information is acquired and when it is used. What's more, the Personal Information at issue may have been available on the Dark Web since 2021. Furthermore, identity monitoring only alerts someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's Personal Information)—it does not prevent identity theft.[24]

60. Plaintiff and Class Members have been damaged in several other ways as well. Plaintiff and Class Members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their Personal Information. Plaintiff and Class Members must now and indefinitely closely monitor their financial and other accounts to guard

---

[23] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited April 4, 2024).

[24] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html (last visited April 4, 2024).

against fraud. This is a burdensome and time-consuming activity. Class Members may have also purchased credit monitoring and other identity protection services, purchased credit reports, placed credit freezes and fraud alerts on their credit reports, and spent time investigating and disputing fraudulent or suspicious activity on their accounts. Plaintiff and Class Members also suffered a loss of the inherent value of their Personal Information.

61. Personal Information stolen in the Data Breach can be misused on its own, or it can be combined with personal information from other sources such as publicly available information, social media, etc., to create a package of information capable of being used to commit further identity theft. Thieves can also use the stolen Personal Information to send spear-phishing emails to Class Members to trick them into revealing sensitive information. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the individual agrees to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

62. As a result of Defendant's failures to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their Personal Information;

b. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

d. The continued risk to their Personal Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Personal Information in their possession;

e. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and

f. Anxiety and distress resulting from fear of misuse of their Personal Information.

63. In addition to a remedy for the economic harm, Plaintiff and Class Members maintain an undeniable interest in ensuring that their Personal Information is secure, remains secure, and is not subject to further misappropriation and theft.

## CLASS ACTION ALLEGATIONS

64. Plaintiff brings this class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of herself and on behalf of all others similarly situated.

65. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

**Nationwide Class**:

**All persons in the United States whose Personal Information was exposed to unauthorized parties as a result of the data breach of AT&T, Inc. that was announced on or around March 30, 2024.**

66. Plaintiff reserves the right to modify, change, or expand the Class definition, including proposing additional subclasses, based on discovery and further investigation.

67. Excluded from the Class are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant has a controlling interest, and its current or former

employees, officers, and directors; (3) counsel for Plaintiff and Defendant; and (4) legal representatives, successors, or assigns of any such excluded persons.

68. The Class meets all of the criteria required by Federal Rule of Civil Procedure 23(a).

69. **Numerosity:** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, it appears that the membership of the Class are in the tens of thousands. The identities of Class members are also ascertainable through Defendant's records.

70. **Commonality:** Common questions of law and fact exist as to all Class Members. These common questions of law or fact predominate over any questions affecting only individual members of the Class. Common questions include, but are not limited to, the following:

a. Whether and to what extent Defendant had a duty to protect the Personal Information of Plaintiff and Class Members;

b. Whether Defendant failed to adequately safeguard the Personal Information of Plaintiff and Class Members;

c. Whether and when Defendant actually learned of the Data Breach;

d. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Personal Information had been compromised;

e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

f. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

g. Whether Defendant was negligent or negligent *per se*;

h. Whether Plaintiff and Class Members are entitled to relief from Defendant as a result of Defendant's misconduct, and if so, in what amounts; and

i. Whether Class Members are entitled to injunctive and/or declaratory relief to address the imminent and ongoing harm faced as a result of the Data Breach.

71. **Typicality:** Plaintiff's claims are typical of the claims of the Class she seeks to represent, in that the named Plaintiff and all members of the proposed Class have suffered similar injuries as a result of the same misconduct alleged herein. Plaintiff has no interests adverse to the interests of the other members of the Class.

72. **Adequacy:** Plaintiff will fairly and adequately protect the interests of the Class and has retained counsel that are well experienced in class actions and complex litigation, including cases alleging breach of privacy and negligence claims arising from corporate misconduct.

73. The Class also satisfies the criteria for certification under Federal Rule of Civil Procedure 23(b) and 23(c). Among other things, Plaintiff avers that the prosecution of separate actions by the individual members of the proposed class would create a risk of inconsistent or varying adjudication which would establish incompatible standards of conduct for Defendant; that the prosecution of separate actions by individual class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other Class Members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; that Defendant has acted or refused to act on grounds that apply generally to the proposed Class, thereby making final injunctive relief or declaratory relief described herein appropriate with respect to the proposed Class as a whole; that questions of law or fact common to the Class predominate over any questions affecting only individual members

and that class action treatment is superior to other available methods for the fair and efficient adjudication of the controversy which is the subject of this action. Plaintiff also avers that certification of one or more subclasses or issues may be appropriate for certification under Federal Rule of Civil Procedure 23(c). Plaintiff further states that the interests of judicial economy will be served by concentrating litigation concerning these claims in this Court, and that the management of the Class will not be difficult.

74. Plaintiff and other members of the Class have suffered damages as a result of Defendant's unlawful and wrongful conduct. Absent a class action, Defendant's unlawful and improper conduct shall, in large measure, go unremedied. Absent a class action, the members of the Class will not be able to effectively litigate these claims and will suffer further losses.

## CLAIMS FOR RELIEF

### COUNT I
**Negligence**

75. Plaintiff realleges each and every allegation contained above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

76. Plaintiff brings this claim on behalf of herself and the Class.

77. Defendant negligently represented that it would safeguard Personal Information despite leaving Plaintiff's and the Class's Personal Information exposed to unauthorized access.

78. Defendant was entrusted with, stored, and otherwise had access to the Personal Information of Plaintiff and Class Members.

79. Defendant knew, or should have known, of the risks inherent to storing the Personal Information of Plaintiff and Class Members, and failed to ensure that its products and services were secure. These risks were reasonably foreseeable to Defendant.

80. Defendant owed duties of care to Plaintiff and Class Members whose Personal Information had been entrusted to them.

81. Further, after discovering its customers' Personal information was on the Dark Web, Defendant failed to timely notify its customers, and, consequently, caused notice to Plaintiff and Class Members to be untimely and insufficient to identify what Personal Information had been exposed.

82. Defendant had additional duties to safeguard Plaintiff's and Class Members' data through the following statutes and regulations:

a. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Personal Information.

83. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Personal Information.

84. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect the Plaintiff's and Class Members' Personal Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Personal Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Allowing unauthorized access to and exfiltration of Plaintiff's and Class Members' Personal Information;

d. Failing to timely detect that Plaintiff's and Class Members' Personal Information had been compromised;

e. Failing to provide timely notice that Plaintiff's and Class Members' Personal Information had been compromised so those at risk could take timely and appropriate steps to mitigate the potential for identity theft and other damages; and

f. Failing to provide adequate notice of what Personal Information had been compromised so that Plaintiff and Class Members at risk could take timely and appropriate steps to mitigate the potential for identify theft and other damages.

85. It was foreseeable to Defendant that its failure to use reasonable measures to protect Plaintiff's and Class Members' Personal Information would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of ransomware attacks and data breaches.

86. It was additionally foreseeable to Defendant that failure to timely and adequately provide notice of the Data Breach would result in Plaintiff and Class Members not being afforded the ability to timely safeguard their identities.

87. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate data security in connection to its services. Defendant had a duty to safeguard Plaintiff's and Class Members' Personal Information and to ensure that their systems and products adequately protected the Personal Information.

88. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

89. Defendant acted with wanton disregard for the security of Plaintiff's and Class Members' Personal Information.

90. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Personal Information.

91. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury, including but not limited to:

- actual identity theft;
- the loss of the opportunity of how their Personal Information is used;
- the compromise, publication, and/or theft of their Personal Information;
- out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information;
- the continued risk to their Personal Information, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Personal Information in its continued possession; and
- future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

92. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members face an increased risk of future harm.

93. Plaintiff is entitled to compensatory and consequential damages suffered as a result of the Data Breach.

94. Plaintiff is also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security programs and monitoring procedures; (ii) submit to future annual

audits of those systems and monitoring procedures; and (iii) immediately provide robust and adequate credit monitoring to all Class members, and any other relief this Court deems just and proper.

95. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members and are entitled to damages in an amount to be proven at trial.

**COUNT II**
**Negligence Per Se**

96. Plaintiff realleges each and every allegation contained above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

97. Plaintiff brings this claim on behalf of herself and the Class.

98. Pursuant to the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, Defendant had a duty to provide adequate data security practices to safeguard Plaintiff's and Class Members' Personal Information.

99. Pursuant to other state and federal laws requiring the confidentiality of Personal Information, including, but not limited to, the FTC Act, among other laws, Defendant had a duty to implement reasonably safeguards to protect Plaintiff's and Class Members' Personal Information.

100. Defendant breached its duties to Plaintiff and Class Members under the FTC Act, among other laws, by failing to provide fair, reasonable, or adequate data security in order to safeguard Plaintiff's and Class Members' Personal Information.

101. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

102. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

103. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that its breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Personal Information.

104. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members face an increased risk of future harm.

105. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

## COUNT III
## Breach of Express and/or Implied Contract

106. Plaintiff realleges each and every allegation contained above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

107. Plaintiff brings this claim on behalf of herself and the Class.

108. Plaintiff and Class Members provided their Personal Information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that Personal Information from unauthorized disclosure.

109. Plaintiff and Class Members are parties to contracts with Defendant. Under the circumstances, recognition of a right to performance by Plaintiff and Class Members is appropriate to effectuate the intentions of the parties to these contracts. One or more of the parties to these contracts intended to give Plaintiff and Class Members the benefit of the performance promised in the contracts.

110. Defendant breached these express and/or implied agreements, which directly and/or proximately caused Plaintiff and Class Members to suffer substantial damages.

111. Accordingly, Plaintiff and Class Members are entitled to damages, restitution, disgorgement of profits, and other relief in an amount to be proven at trial.

**COUNT IV**
**Invasion of Privacy**

112. Plaintiff realleges each and every allegation contained above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

113. Plaintiff brings this claim on behalf of herself and the Class.

114. Plaintiff and Class Members had a legitimate and reasonable expectation of privacy with respect to their Personal Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

115. Defendant owed a duty to its customers, including Plaintiff and Class Members, to keep their Personal Information confidential.

116. The unauthorized release of Personal Information, especially Social Security numbers, is highly offensive to a reasonable person.

117. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their Personal Information to Defendant as part of their use of Defendant's services, but privately, with the intention that the Personal Information would be kept confidential and protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

118. The Data Breach constitutes an intentional interference with Plaintiff's and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

119. Defendant acted with a knowing state of mind when they permitted the Data Breach because it knew its information security practices were inadequate and would likely result in a data breach such as the one that harmed Plaintiff and Class Members.

120. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and Class Members.

121. As a proximate result of Defendant's acts and omissions, Plaintiff's and Class Members' Personal Information was disclosed to and used by third parties without authorization in the manner described above, causing Plaintiff and Class Members to suffer damages.

122. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the Personal Information maintained by Defendant can be viewed, distributed, and used by unauthorized persons.

123. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

## COUNT V
## Declaratory Judgement

124. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

125. Plaintiff brings this claim on behalf of herself and the Class.

126. Plaintiff and the Class have stated claims against Defendant for common law torts.

127. Defendant failed to fulfill its obligations to provide adequate and reasonable data security measures for the Personal Information of Plaintiff and the Class, as evidenced by the Data Breach.

128. As a result of the Data Breach, Defendant's systems are more vulnerable to access by unauthorized parties and require more stringent measures to be taken to safeguard the Plaintiff's and Class Members' Personal Information going forward.

129. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's current obligations to provide data security measures that will adequately protect Plaintiff's and Class Members' Personal Information.

130. Plaintiff seeks a declaration that Defendant must implement specific additional, prudent, industry-standard data security practices to provide reasonable protection and security to Plaintiff and Class Members' Personal Information. Specifically, Plaintiff and the Class seek a declaration that Defendant's existing security measures do not comply with its obligations, and that Defendant must implement and maintain reasonable data security measures on behalf of Plaintiff and the Class to comply with its data security obligations.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and on behalf of the Class, prays for relief as follows:

A. For an Order certifying this case as a class action pursuant to Federal Rule of Civil Procedure 23 against Defendant, and appointing Plaintiff as Class Representative of the Class;

B. Awarding monetary, punitive, and actual damages and/or restitution, as appropriate;

C. Awarding declaratory and injunctive relief as permitted by law or equity to assure that the Class have an effective remedy, including enjoining Defendant from continuing the unlawful practices as set forth above;

D. Pre-judgment interest to the extent allowed by the law;

E. Awarding all costs, experts' fees, attorneys' fees, expenses, and costs of prosecuting this action; and

F. Such other and further relief as the Court may deem just and proper.

**JURY TRIAL DEMAND**

Plaintiff demands a trial by jury on all issues so triable.

Respectfully submitted,

DATED: April 8, 2024

**LYNN PINKER HURST & SCHWEGMANN, LLP**

By: *Michael K. Hurst*

Michael K. Hurst
State Bar No. 10316310
mhurst@lynnllp.com
Rebecca L. Adams
State Bar No. 24098255
radams@lynnllp.com
Yaman Dasai
State Bar No. 24101695
ydesai@lynnllp.com
Jessica D. Cox
State Bar No. 24114769
jcox@lynnllp.com

2100 Ross Avenue, Suite 2700
Dallas, Texas 75201
Telephone: (214) 981-3800
Facsimile: (214) 981-3839

**THE PETTIT LAW FIRM**
Julie Pettit
State Bar No. 24065971
jpettit@pettitfirm.com
2101 Cedar Springs, Suite 1540
Dallas, Texas 75201
Telephone: (214) 329-0151
Facsimile: (214) 329-4076

**KAPLAN FOX & KILSHEIMER LLP**
Laurence D. King (*pro hac vice* forthcoming)
Matthew B. George (*pro hac vice* forthcoming)
Blair E. Reed (*pro hac vice* forthcoming)
Clarissa R. Olivares (*pro hac vice* forthcoming)
1999 Harrison Street, Suite 1560
Oakland, CA 94612
Telephone: 415-772-4700
Facsimile: 415-772-4707
Email: *lking@kaplanfox.com*
*mgeorge@kaplanfox.com*
*breed@kaplanfox.com*
*colivares@kaplanfox.com*

*Attorneys for Plaintiff and the Proposed Class*